QSC 18

QUALYS SECURITY CONFERENCE 2018

Qualys Container Security

Comprehensive Security for the ever-changing Container Stack

Asif Awan
CTO, Container Security, Qualys, Inc.

Agenda

Container Advantages

Container Deployments

Visibility & Control Challenges

Qualys Container Security Solution

Demo

Q&A

Everybody Loves Containers

Portability

Agility

Density

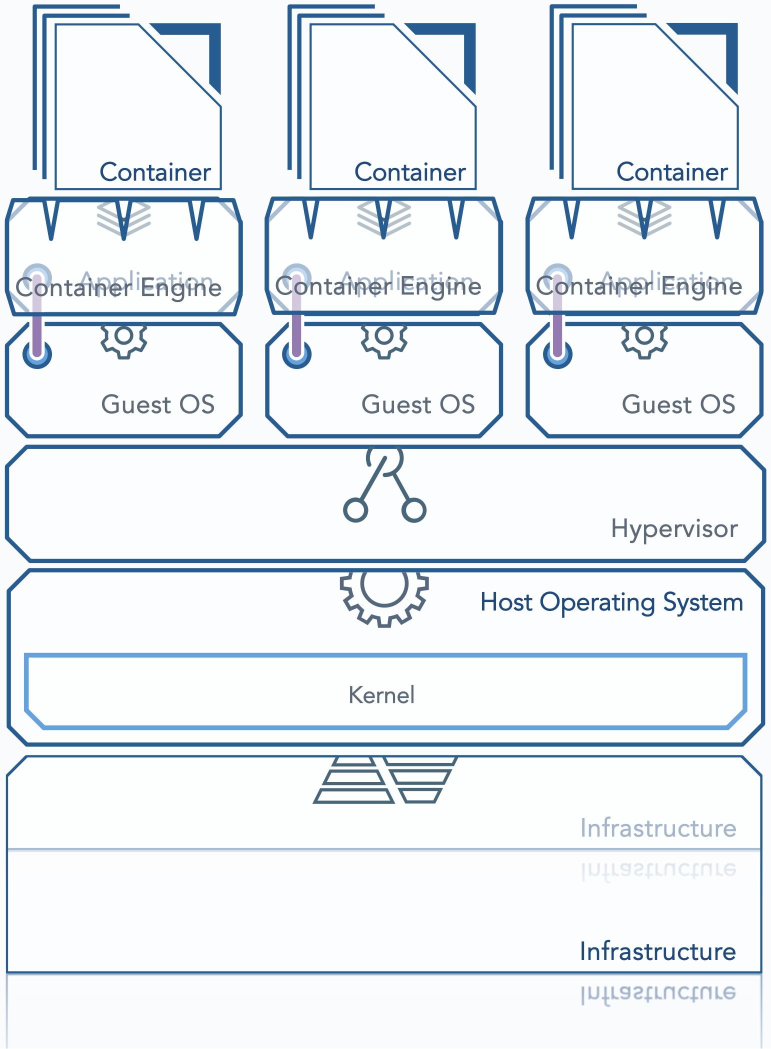
Container Deployments

Qualys.

Deployment Scenario #1

Use Case

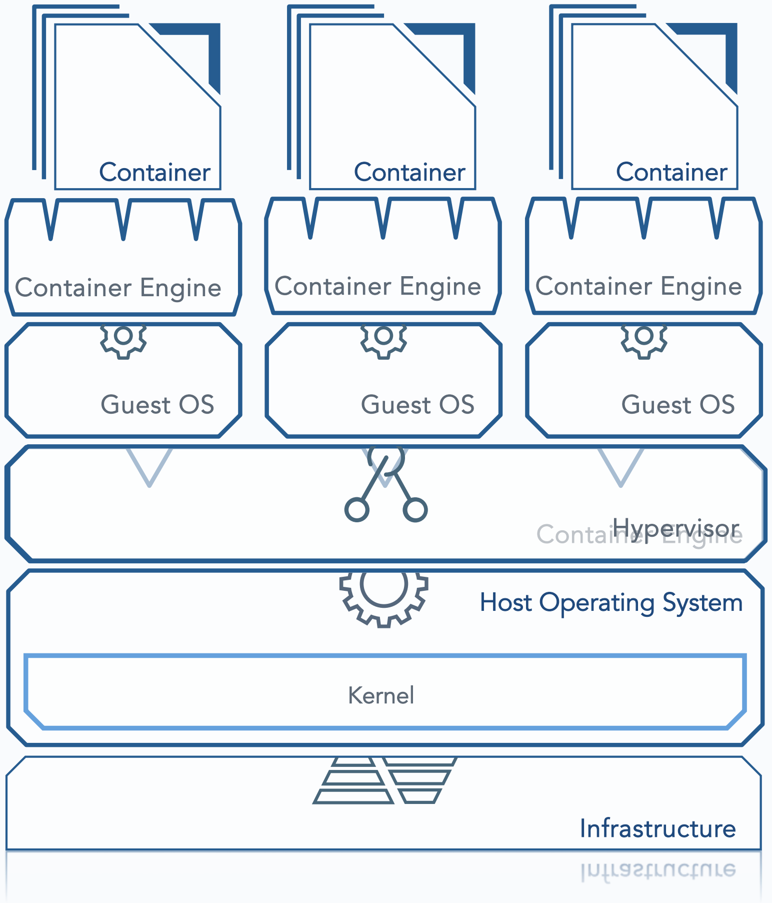
1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines



Deployment Scenario #2

Use Case

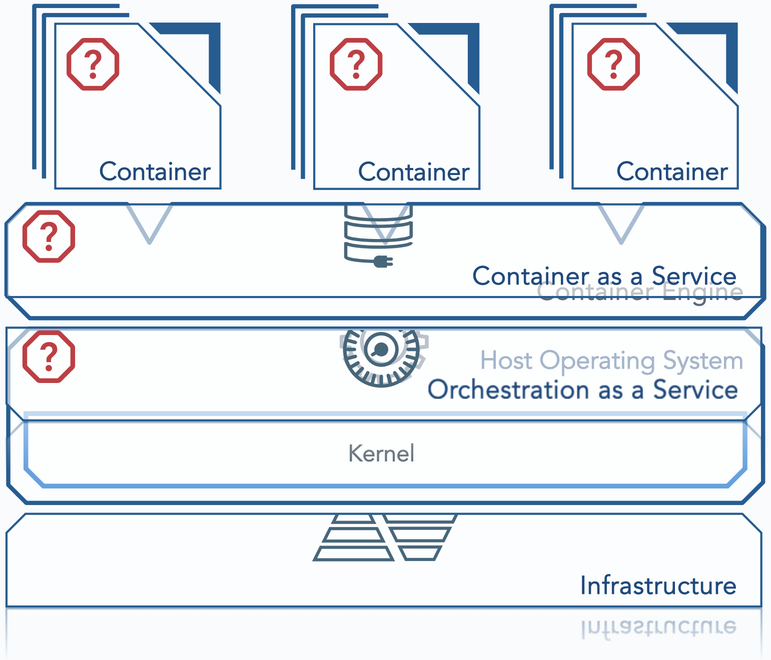
1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters



Deployment Scenario #3

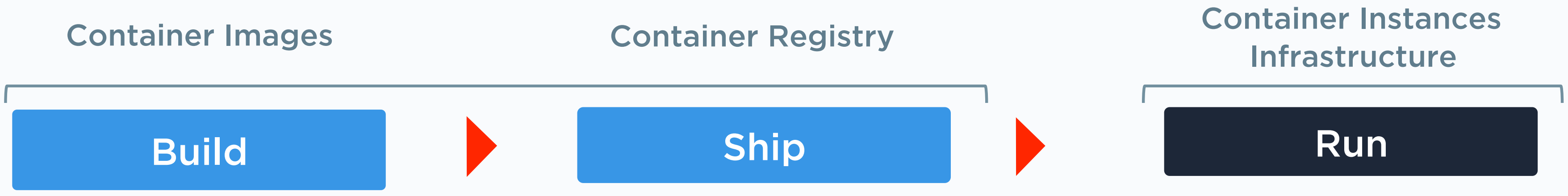
Use Case

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?



Container Visibility & Security Challenges

Container Lifecycle Challenges



Build

What’s in the images?

Vulnerabilities?

OSS license exposure?

Solution disruptive to my CI Pipeline?

Scanning report integrated with bug tracking?

Ship

Registry scanning?

Enforce compliance?

Vulnerability, package and license-based rules?

Vulnerability impact notifications?

Run

How to protect host?

Container engine configured correctly?

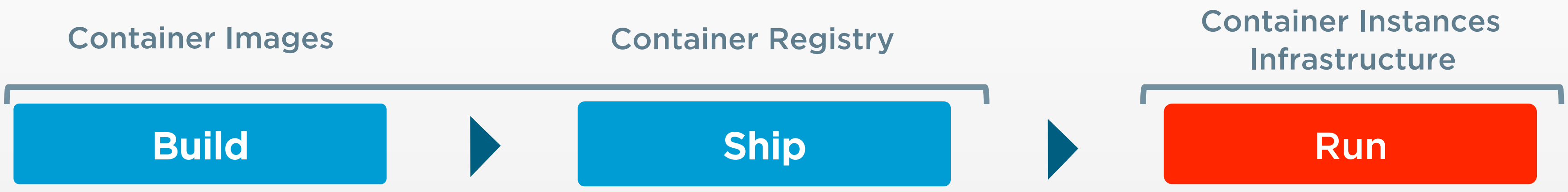
Container orchestration configured correctly?

Runtime app visibility?

Runtime app protection?

Qualys Container Security

Qualys Container Security



Container Images

Container Registry

Container Instances
Infrastructure

Build

Ship

Run

Software Composition

Vulnerability Analysis

OSS License Analysis

Integration with CI Pipelines

Bug Tracking Integration

Registry Scanning

Compliance Controls

Vulnerability, Package and License-based Rules

Real-time Vulnerability Impact Notifications

Host Protection

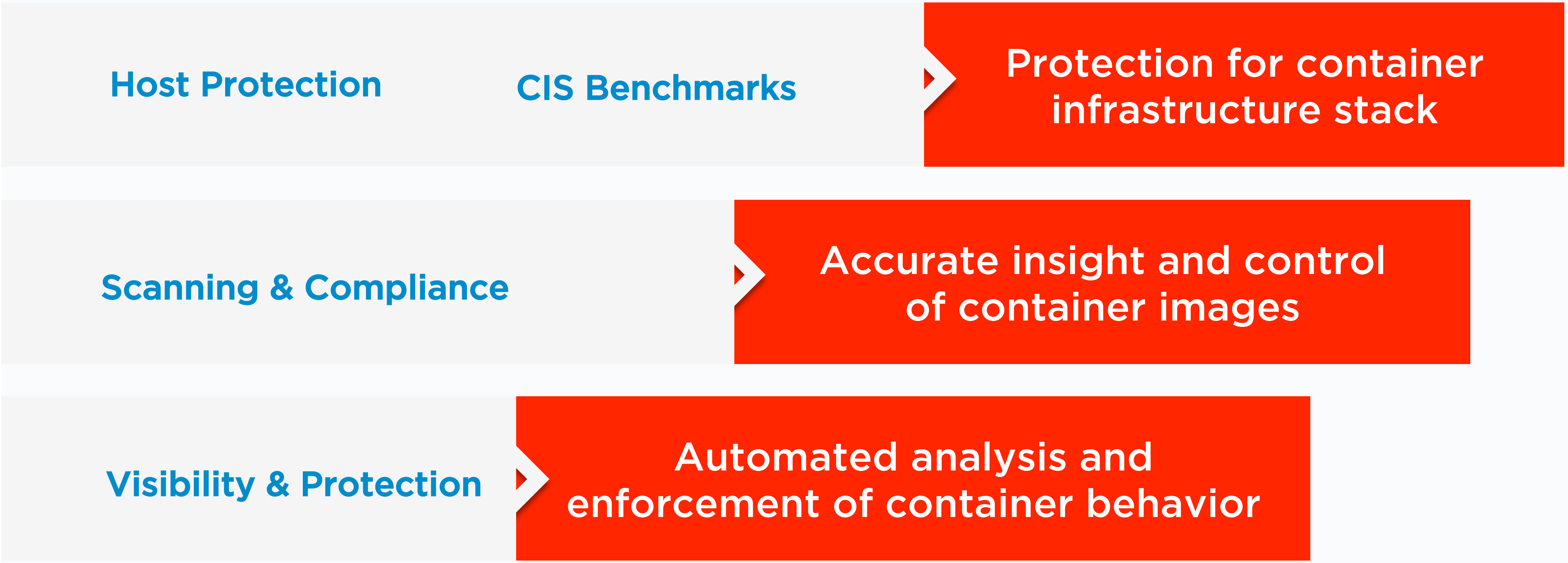
Container Engine Benchmarking

Container Orchestration Benchmarking

Deep Runtime Visibility

Runtime Protection

Qualys Container Security



Host Protection

CIS Benchmarks

Protection for container infrastructure stack

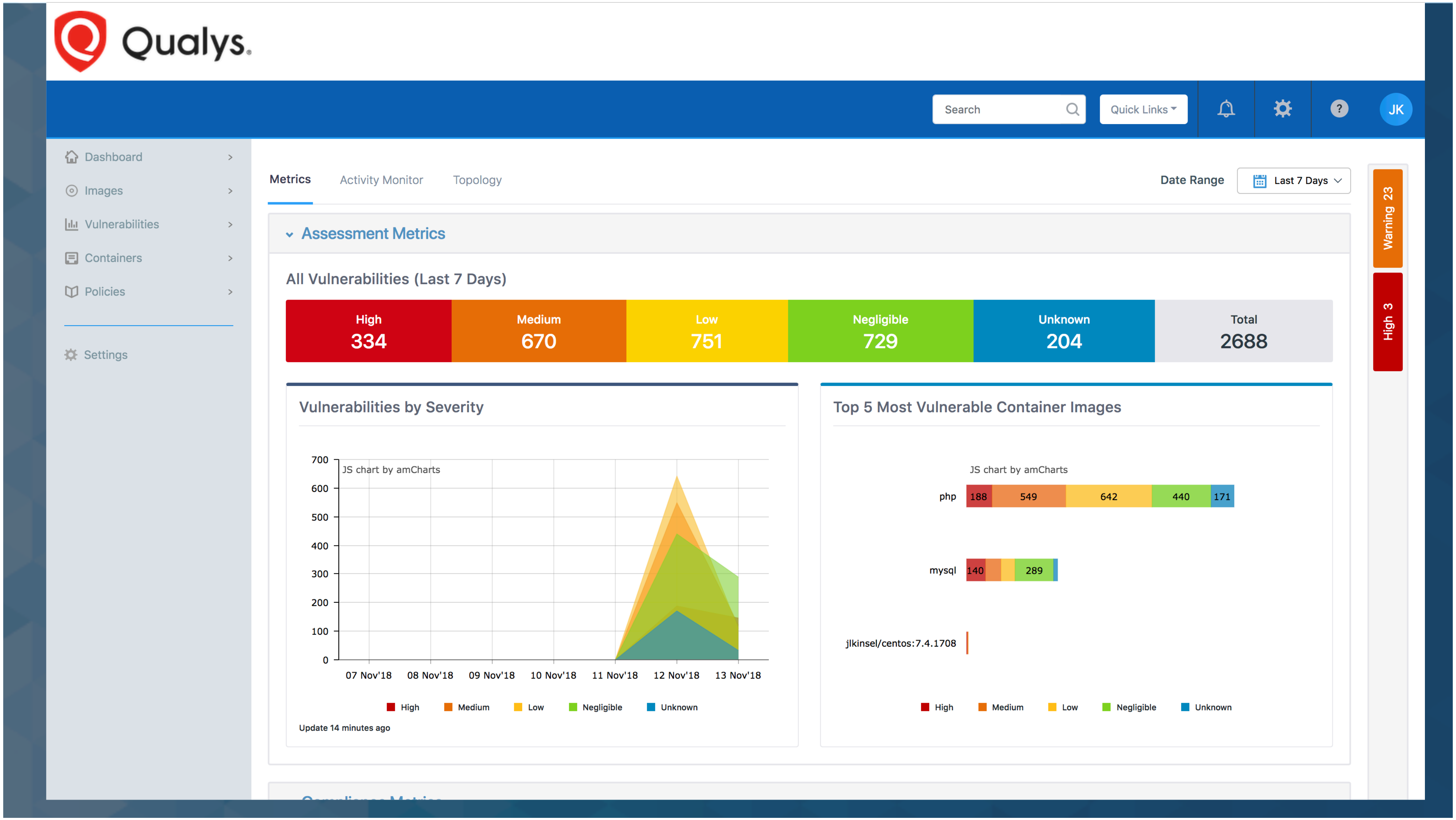
Scanning & Compliance

Accurate insight and control of container images

Visibility & Protection

Automated analysis and enforcement of container behavior

Demo



Assessment Metrics

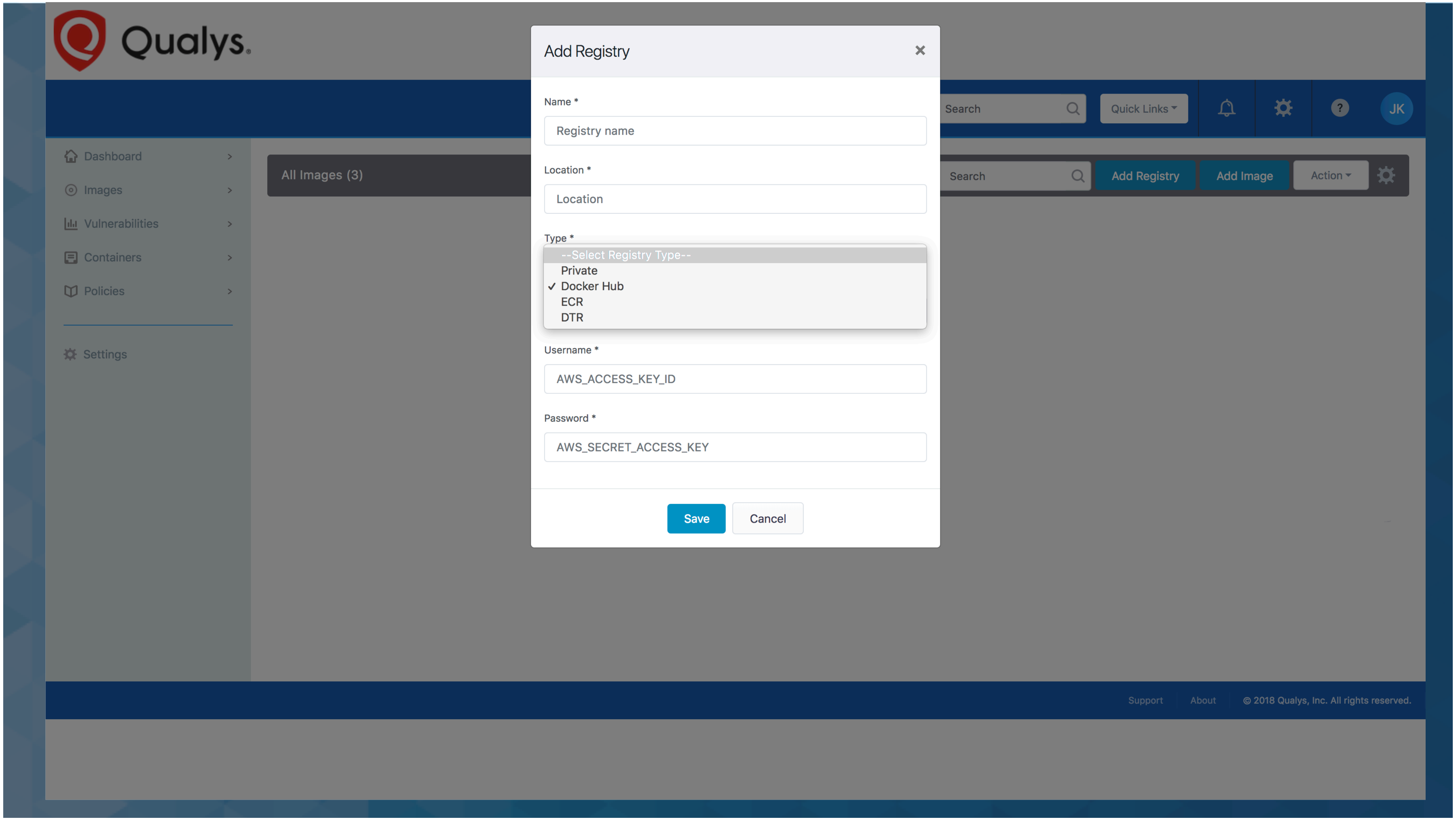
All Vulnerabilities (Last 7 Days)

High	Medium	Low	Negligible	Unknown	Total
334	670	751	729	204	2688

Vulnerabilities by Severity

Update 14 minutes ago

Top 5 Most Vulnerable Container Images



Add Registry ×

Name *

Registry name

Location *

Location

Type *

--Select Registry Type--
Private
✓ Docker Hub
ECR
DTR

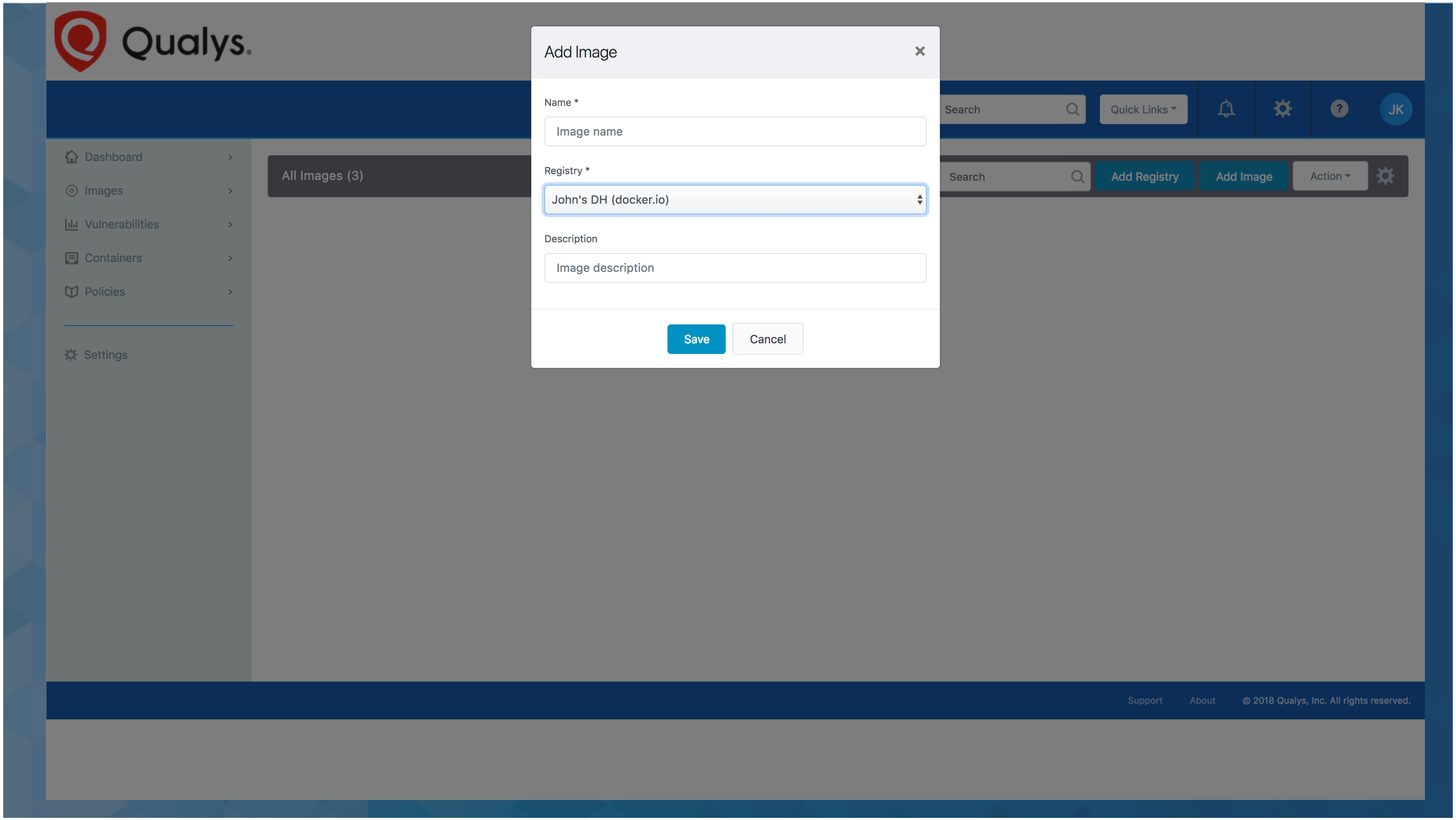
Username *

AWS_ACCESS_KEY_ID

Password *

AWS_SECRET_ACCESS_KEY

Save Cancel



Add Image

Name *

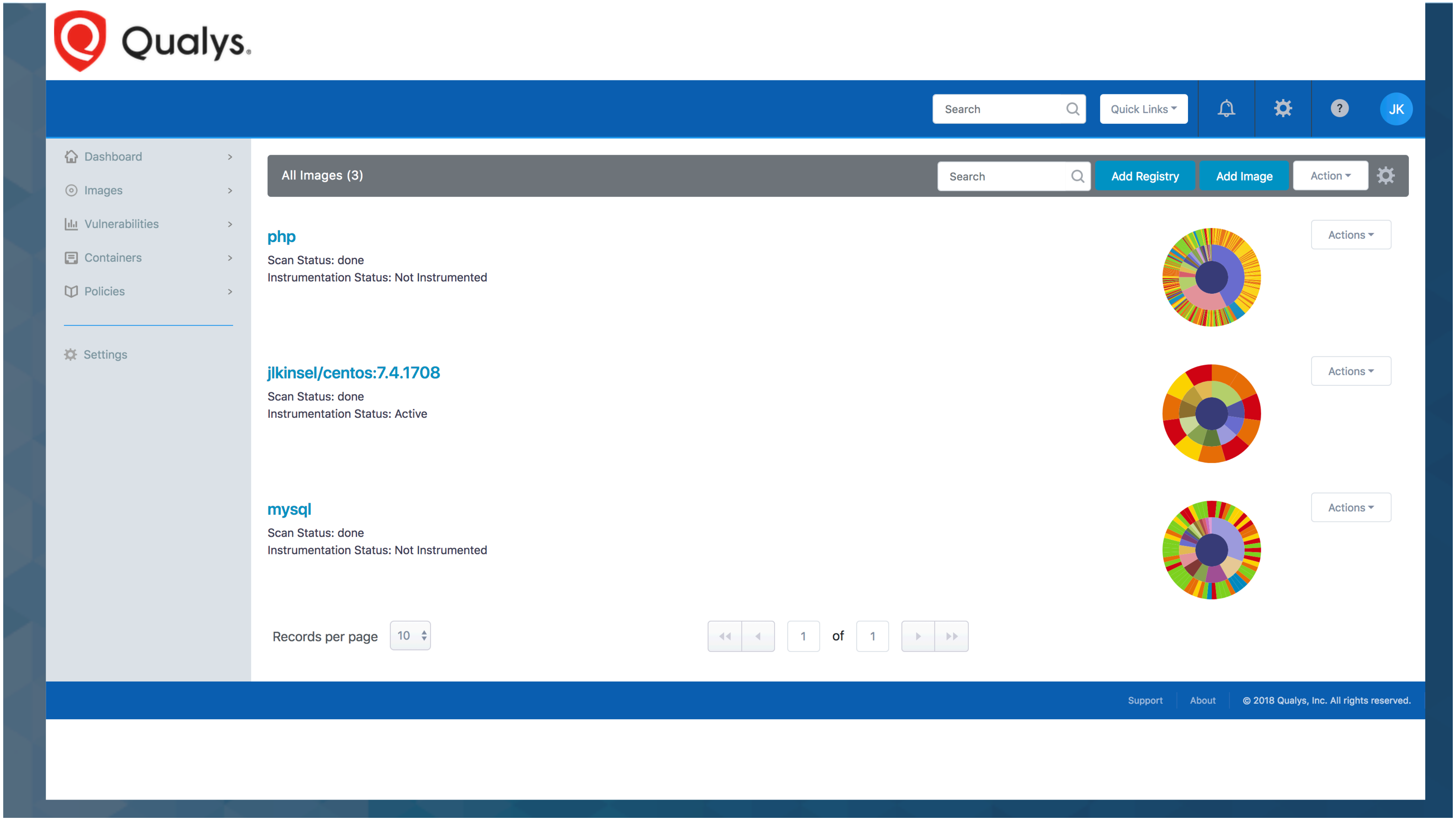
Image name

Registry *

John's DH (docker.io)

Description

Image description



All Images (3)

php
Scan Status: done
Instrumentation Status: Not Instrumented

jlkinsel/centos:7.4.1708
Scan Status: done
Instrumentation Status: Active

mysql
Scan Status: done
Instrumentation Status: Not Instrumented

Records per page 10

1 of 1

© 2018 Qualys, Inc. All rights reserved.

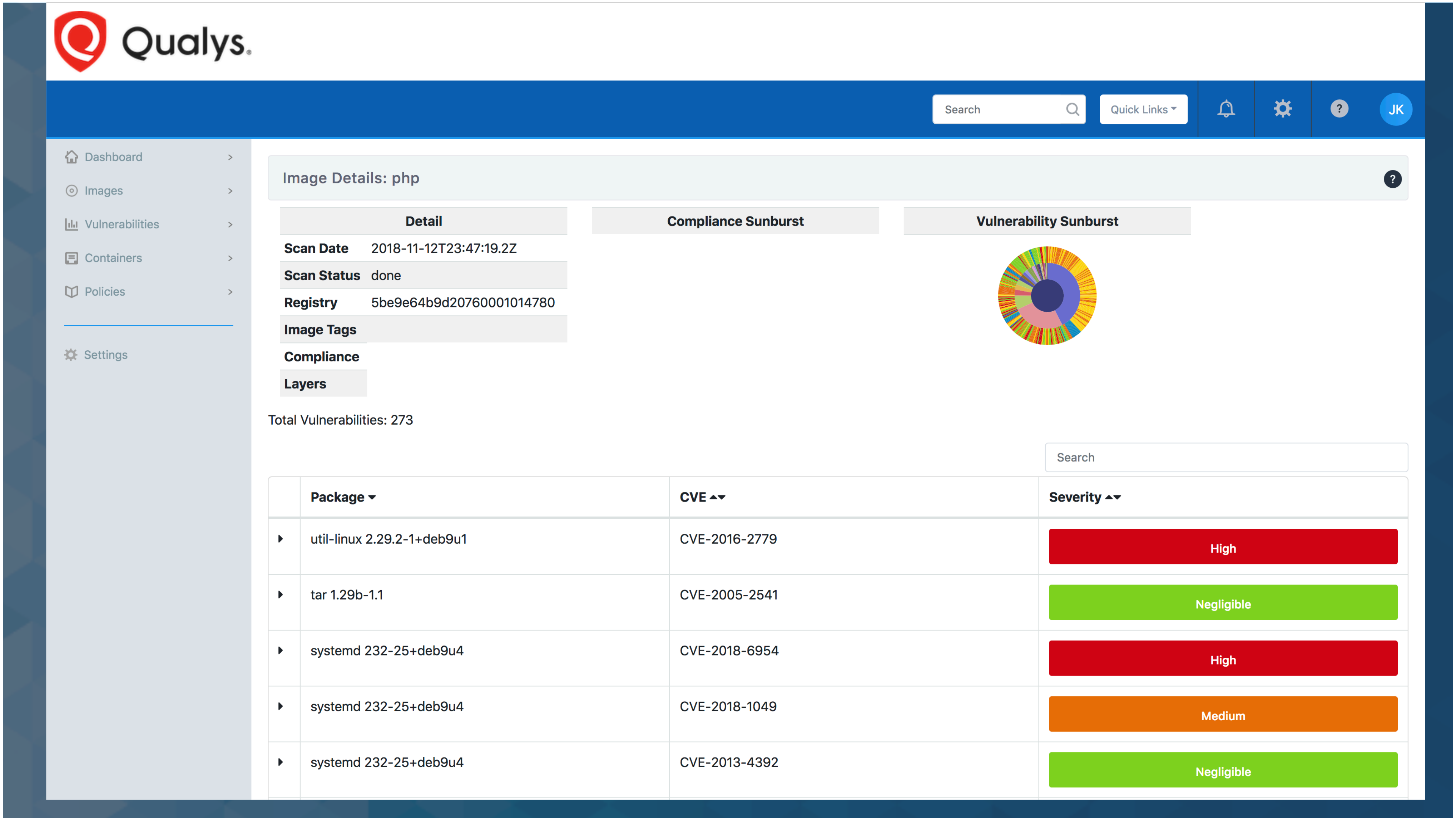


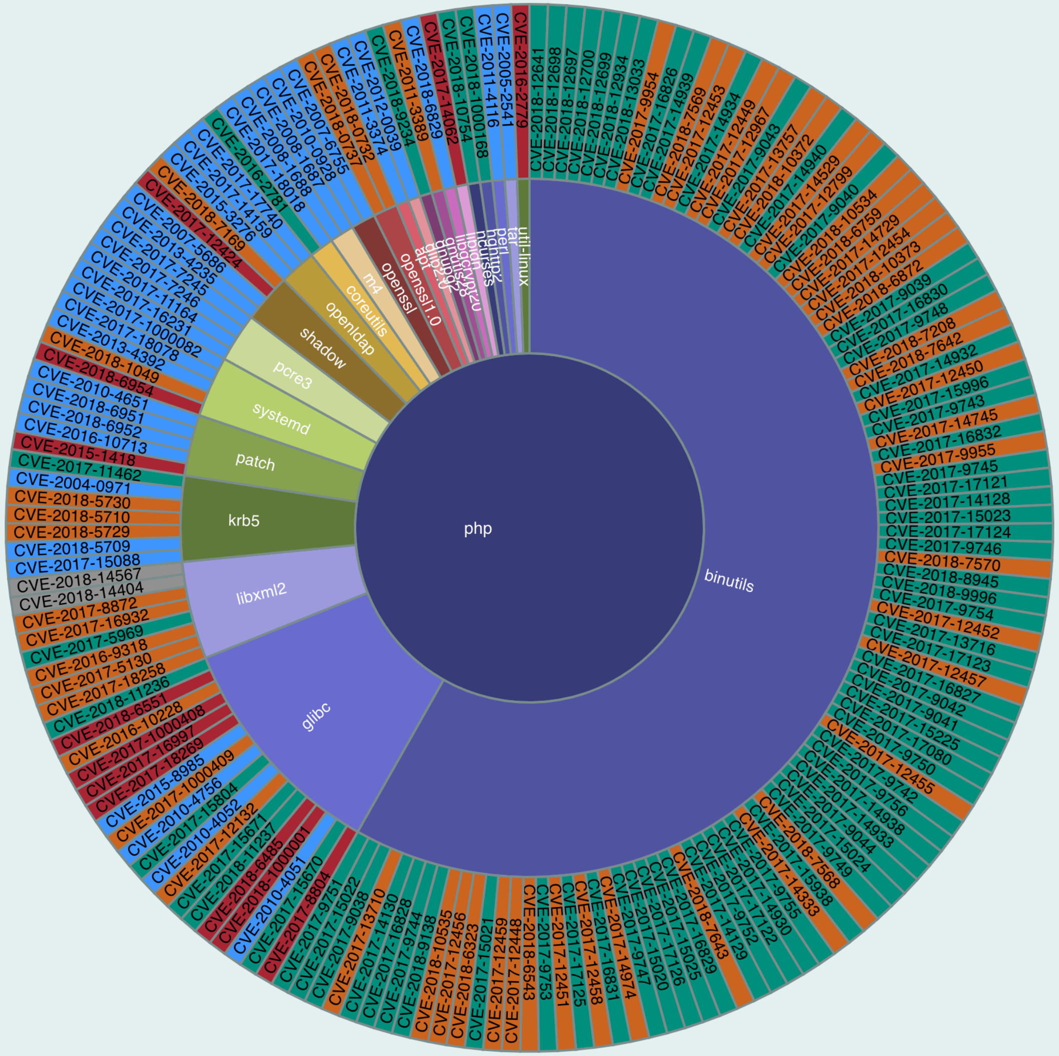
Image Details: php

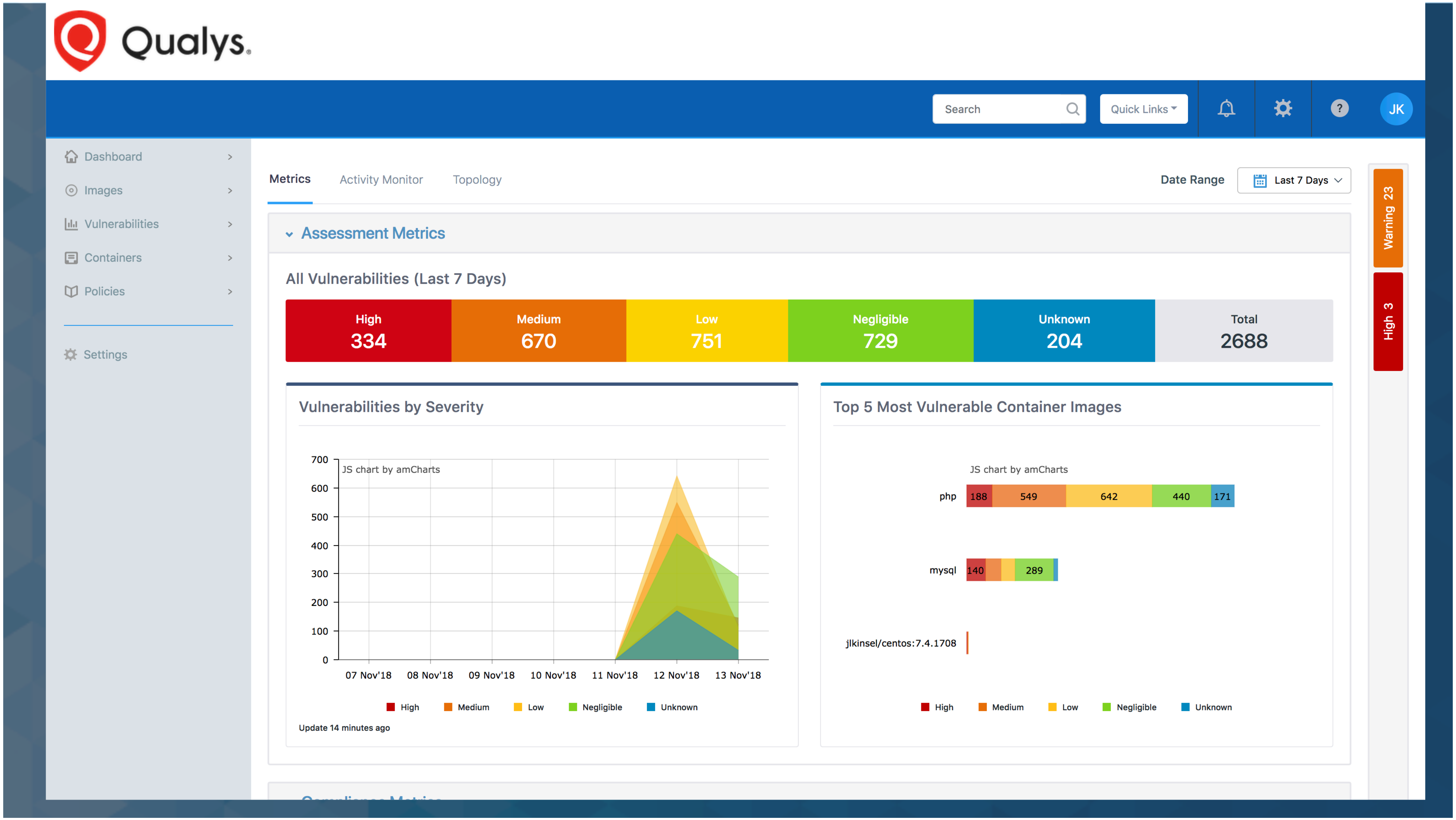
Detail	
Scan Date	2018-11-12T23:47:19.2Z
Scan Status	done
Registry	5be9e64b9d20760001014780
Image Tags	
Compliance	
Layers	

Total Vulnerabilities: 273

Package	CVE	Severity
util-linux 2.29.2-1+deb9u1	CVE-2016-2779	High
tar 1.29b-1.1	CVE-2005-2541	Negligible
systemd 232-25+deb9u4	CVE-2018-6954	High
systemd 232-25+deb9u4	CVE-2018-1049	Medium
systemd 232-25+deb9u4	CVE-2013-4392	Negligible

Vulnerability Sunburst of php





Assessment Metrics

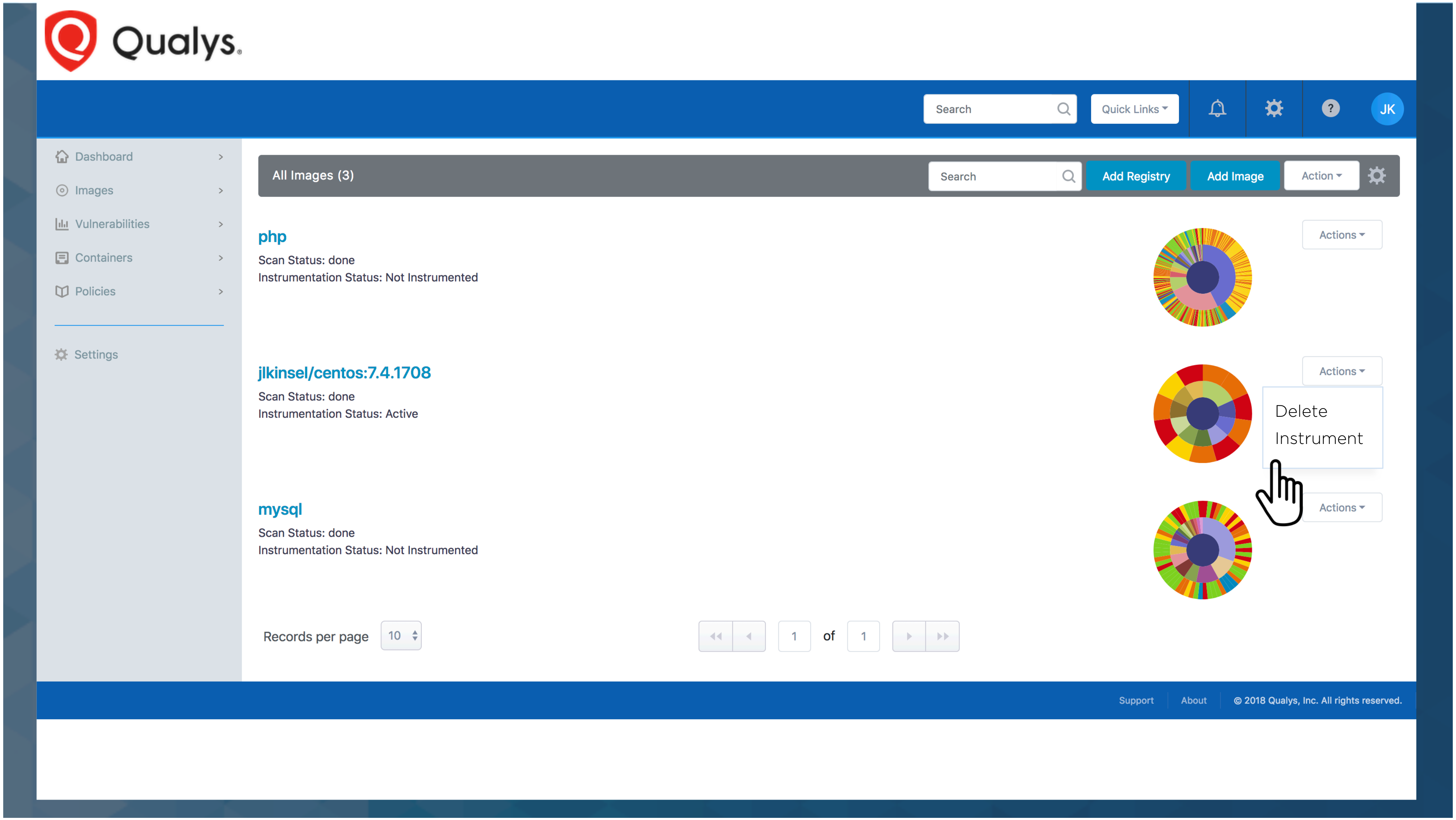
All Vulnerabilities (Last 7 Days)

High	Medium	Low	Negligible	Unknown	Total
334	670	751	729	204	2688

Vulnerabilities by Severity

Update 14 minutes ago

Top 5 Most Vulnerable Container Images



All Images (3)

php
Scan Status: done
Instrumentation Status: Not Instrumented

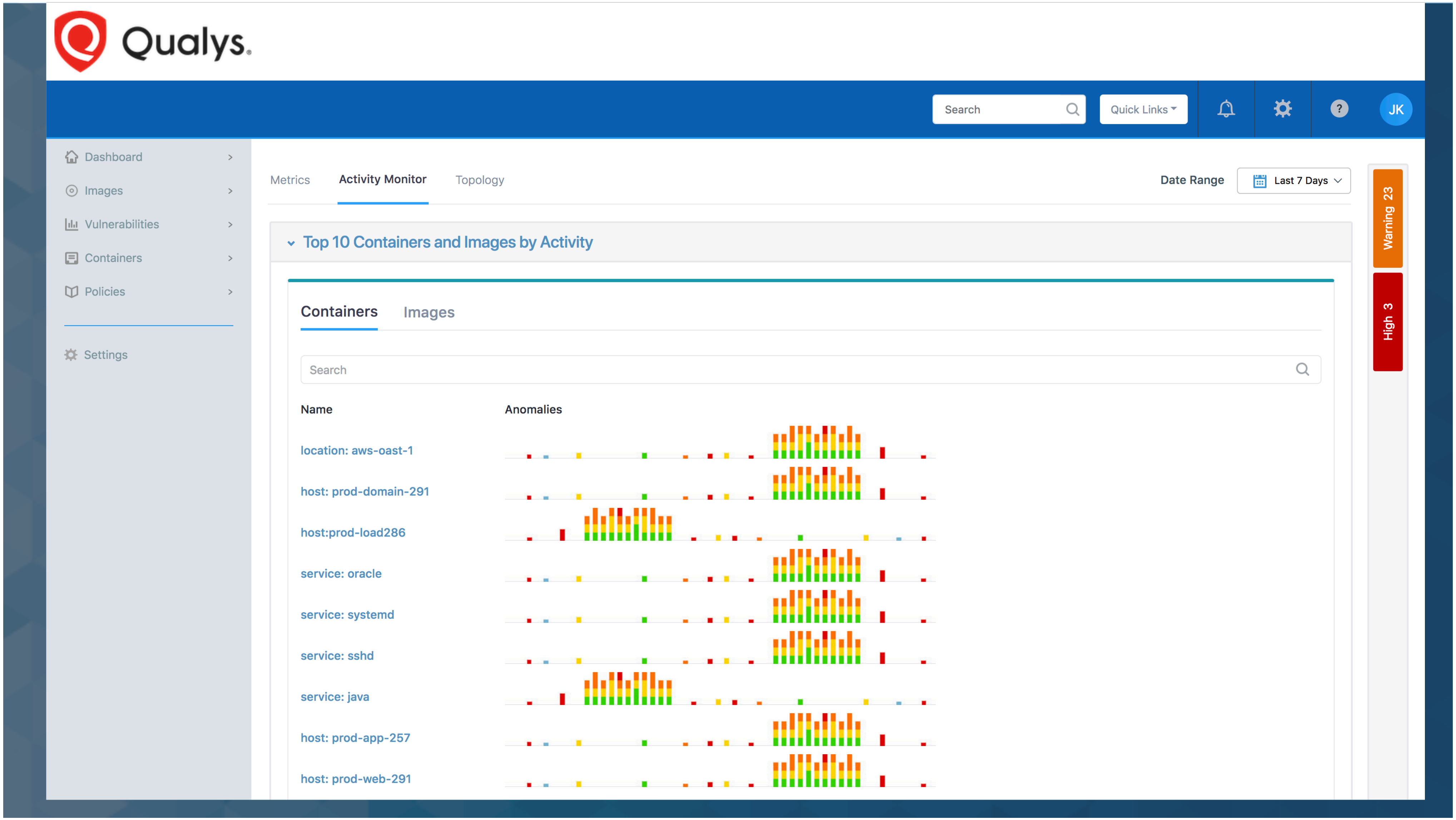
jlkinsel/centos:7.4.1708
Scan Status: done
Instrumentation Status: Active

mysql
Scan Status: done
Instrumentation Status: Not Instrumented

Records per page 10

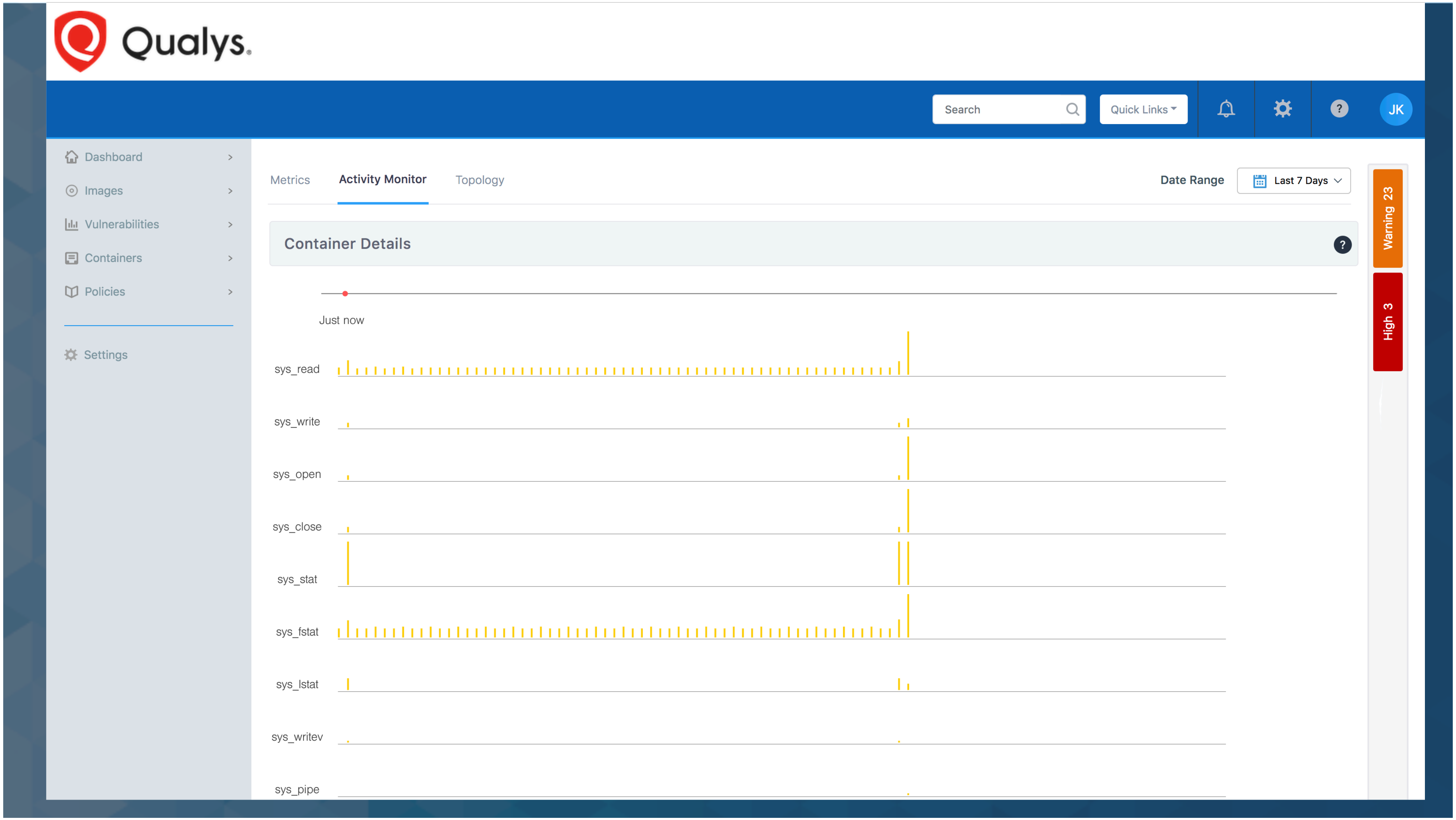
1 of 1

© 2018 Qualys, Inc. All rights reserved.



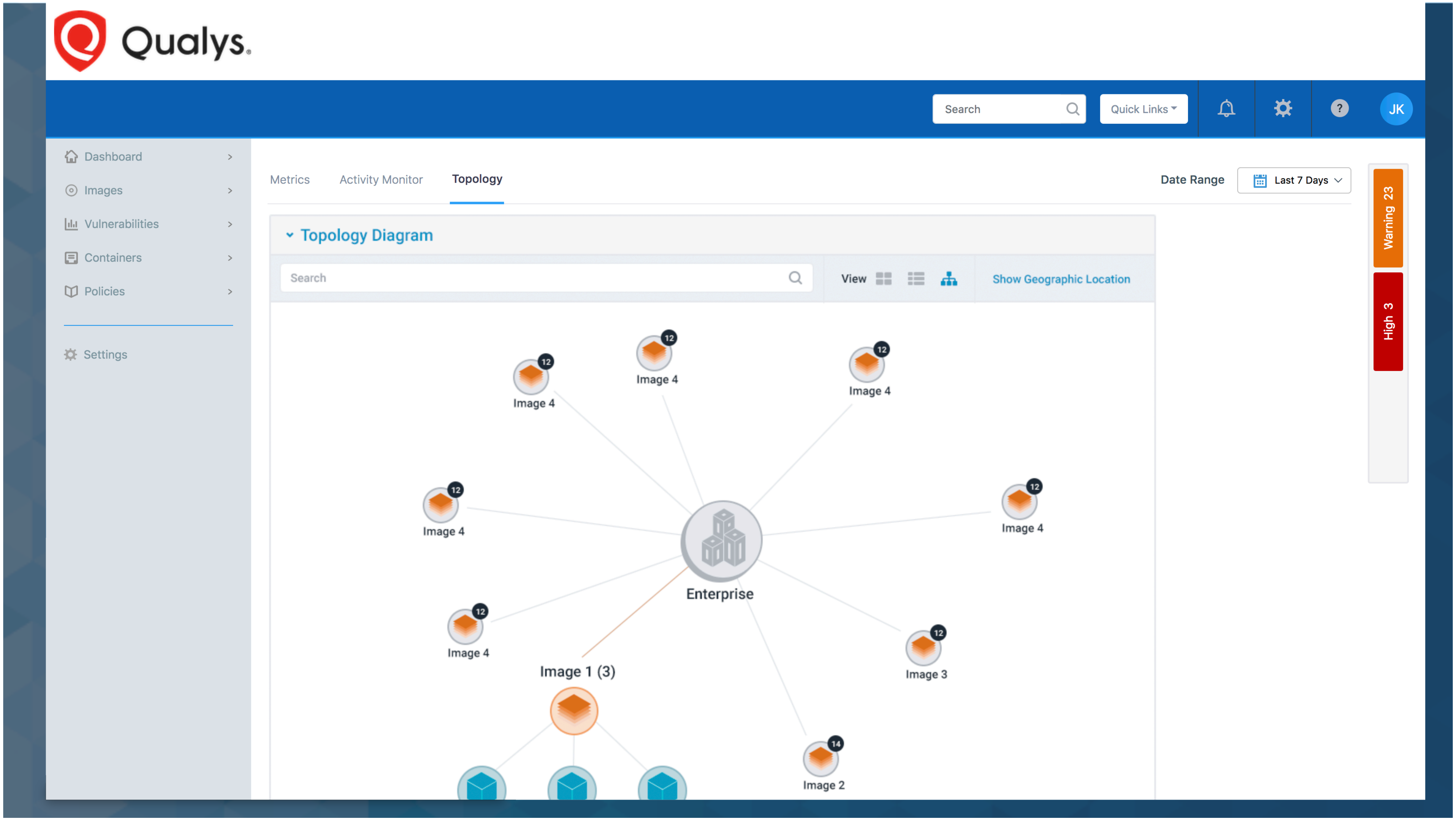
Top 10 Containers and Images by Activity

Name	Anomalies
location: aws-oast-1	
host: prod-domain-291	
host:prod-load286	
service: oracle	
service: systemd	
service: sshd	
service: java	
host: prod-app-257	
host: prod-web-291	

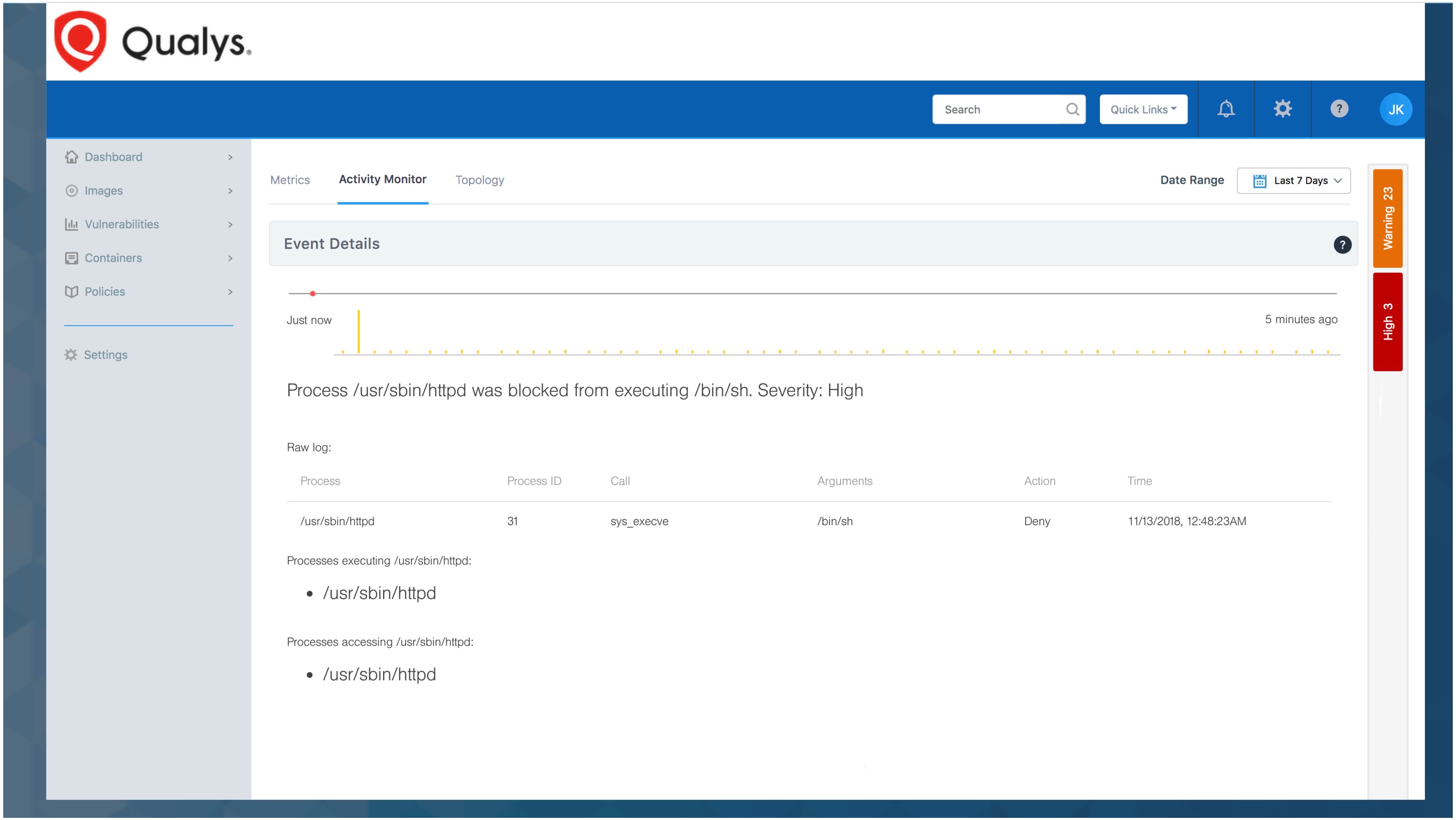


Date Range: Last 7 Days

Container Details



Date Range: Last 7 Days



Event Details

Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

Process	Process ID	Call	Arguments	Action	Time
/usr/sbin/httpd	31	sys_execve	/bin/sh	Deny	11/13/2018, 12:48:23AM

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd

Thank You

Asif Awan
aawan@qualys.com